Defense Logistics Agency
INSTRUCTION

DLAI 8510.01
Effective July 21, 2014

JC1

SUBJECT: Information Assurance (IA) Management Controls

References: Refer to Enclosure 1

1. PURPOSE. This instruction reissues and cancels DLAI 6401 (Reference (a)) to update established policy, assigned responsibilities, and requirements to implement, manage, and sustain an effective Defense Logistics Agency (DLA) IA Program. It defines IA policy requirements, roles and responsibilities to ensure implementation of IA management controls through a defense-in-depth approach that integrates the processes and objectives associated with: IA risk management, system development life cycle management, IA Certification and Accreditation (C&A), change management/configuration management (CM), IA policy development, IA workforce improvement, and IA Compliance Review Program management and execution.

2. APPLICABILITY. This instruction applies to all DLA Activities.

3. DEFINITIONS. Refer to Glossary.

4. POLICY. It is DLA policy:

a. To comply with DOD Instruction (DODI) 8500.01 (Reference (b)), to implement, manage and sustain an Agency-level IA Program.

b. To accredit and certify its information systems utilizing the Defense Information Systems Agency (DISA) sponsored eMASS. Unless otherwise specified, all DIACAP packages shall be submitted via eMASS which is fully implemented on both the DLA Non-Classified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet).

c. To begin transitioning to the Risk Management Framework per DODI 8510.01 (Reference (c)) within six months.

5. RESPONSIBILITIES. Refer to Enclosure 2.

6. PROCEDURES. Refer to Enclosure 3.

7. INTERNAL CONTROLS. The certification and accreditation of the information system from development through review and approval of the accreditation package is performed within the Enterprise Mission Support Service (eMASS) system. The DAA digitally signs the scorecard within eMASS documenting the accreditation decision for an information system.

8. RELEASIBILITY. UNLIMITED. This instruction is approved for public release and is available on the Internet from the DLA Issuances Internet Website.

9. EFFECTIVE DATE. This Instruction:

a. Is effective on July 21, 2014.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DLAI 5025.01, (Reference (d)). If not, it will expire effective July 21, 2024 and be removed from the DLA Issuances Website.

GOLDENBERG.PHYLLISA.S.1229115878
Digitally signed by GOLDENBERG.PHYLLISA.S.1229115878
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DLA, cn=GOLDENBERG.PHYLLISA.S.1229115878
Date: 2014.07.21 12:42:03 -04'00'

PHYLLISA S. GOLDENBERG
Director, DLA Strategic Plans and Policy

Enclosures(s)
Enclosure 1 – References
Enclosure 2 – Responsibilities
Enclosure 3 – Procedures
Glossary

ENCLOSURE 1

REFERENCES

(a) DLA Instruction 6401, "Information Assurance (IA) Management Controls," June 14, 2006 (hereby cancelled)
(b) DOD Instruction 8500.01, "Cybersecurity," March 14, 2014[1]
(c) DOD Instruction 8510.01, "Risk Management Framework (RMF) for DOD Information Technology (IT)," March 12, 2014.
(d) DLA Instruction 5025.01, "DLA Issuance Program," January 4, 2013
(e) DOD Manual 8570.01-M, "Information Assurance Workforce Improvement Program (WIP)," December 19, 2005 (Incorporating Change 3, January 24, 2012)
(f) 44 U.S.C. 3541 - 3549 (2014). Federal Information Security Management Act of 2002
(g) "DLA DIACAP Implementation Guide," Version 2.0, October 5, 2012
(h) DLA Instruction 6404, "Information Assurance (IA) Rules of Behavior," April 16, 2007 (Certified Current February 17, 2012)
(i) DoD 5200.2-R, "Personnel Security Program," January 1987

[1] DLA recognizes the updated DODI 8500.01 and DODI 8510.01 and will adhere to the transition timeline identified of three years and six months. During this timeframe, DLA will require the continuing adherence to the DOD Information Assurance Certification and Accreditation Process (DIACAP).

ENCLOSURE 2

RESPONSIBILITIES

1. DLA DIRECTOR. The DLA Director shall:

a. Appoint the DLA Information Operations (J6) Director/Chief Information Officer (CIO) as the Designated Accrediting Authority (DAA) for all DLA information systems.

b. Ensure the DAA has the level of authority commensurate with accepting the risk of operating all information systems under his/her purview.

2. DLA DAA (J6 DIRECTOR/CIO). The DLA DAA shall:

a. Ensure that all applicable IA related positions are assigned in writing (i.e., appointment memorandums) in accordance with Reference (b) and DOD Manual 8570.01-M (Reference (e)).

b. Appoint the J6 Deputy Director as the alternate DAA. The alternate DAA appointment shall be done in writing. The roles and responsibilities of the alternate DAA shall be acknowledged by the appointee through his/her signature.

c. Appoint the J6, IA (J61) Staff Director as the DLA Senior Information Assurance Officer (SIAO) to direct and coordinate the DLA IA program in accordance with Federal Information Security Management Act (FISMA) (Reference (f)). The DLA SIAO appointment shall be done in writing. The terms of the DLA SIAO appointment shall be acknowledged by the appointee through his/her signature.

d. Appoint all Certifying Authority (CA) Representatives in writing to include requiring appointed CA Representatives to acknowledge their roles and responsibilities through signature. In accordance with the "DLA DOD Information Assurance Certification and Accreditation Process (DIACAP) Implementation Guide" (Reference (g)), the appointment of CA Representative authority and responsibility shall be limited to the responsible J6 Director (if applicable), information technology (IT) chief, or business area manager. This includes the appointment of applicable J6 personnel alternate CA Representatives.

e. Appoint all Information Assurance Managers (IAM) in writing to include requiring all appointees to acknowledge their assigned roles and responsibilities through signature. All appointed IAM's shall annually acknowledge their assigned roles and responsibilities through signature.

f. Verify that a Program Manager or System Manager (PM/SM) is identified for each DLA information system.

g. Ensure that a DIACAP package is initiated and completed for all applicable information systems via eMASS.

3. SIAO. The SIAO shall:

a. Direct and coordinate a DLA IA Program to ensure consistency and compliance with DOD IA directives, instructions, manuals, regulations, and official memoranda. The IA Program components shall include IA policy development and compliance oversight, IA risk management, enclave boundary defense, C&A, IA Workforce Improvement Program (WIP) implementation, and IA Compliance Review Program management.

b. Develop, implement, and manage the Agency's C&A Program.

(1) Serve as the CA for all DLA information systems undergoing C&A.

(2) As the Agency's technical C&A expert, ensure DLA participation in the DIACAP Technical Advisory Group (TAG) and associated working groups.

(3) Monitor the accreditation status of all information systems accredited by the DLA DAA.

(4) Ensure that an IT Security Plan of Action and Milestones (POA&M) Tracking Program is established and managed to provide CA level oversight of an information system's corrective actions status in association with an accreditation decision.

(5) Maintain a current list of all appointed DLA CA Representatives and IAM's, along with the corresponding appointment memorandums endorsed by the DLA DAA.

c. Ensure the IA certification (e.g., Certified Information System Security Professional (CISSP), Security+ CE, etc.,) status of all J6 personnel with IA related job function(s) is tracked and compiled in support of DLA's IA WIP management.

d. Ensure an enterprise DLA IA architecture is developed and documented based on the identified IT resources employed throughout the enterprise. The DLA IA architecture in accordance with DOD standards for configuration and implementation (e.g., DISA Security Technical Implementation Guides (STIG's), United States Cyber Command (USCYBERCOM) guidance, etc.) shall serve as the basis for assessing the Agency's overall IA posture, including the identification of weaknesses and allocation resources for additional IA controls, where applicable.

e. Ensure the completion of outstanding tasks required to correct or satisfactorily mitigate the risk(s) posed by weaknesses identified in POA&M's for information systems accredited by the DLA DAA.

4. CA REPRESENTATIVE. The CA Representative shall:

a. Ensure that applicable IA control requirements are identified, implemented, and continuously monitored for all information systems under their purview.

b. Maintain IA-related, situational awareness of information systems under his/her purview. This includes ensuring POA&M development, tracking, and resolution.

c. Be responsible for providing the DLA CA with a certification recommendation based on the overall reliability and viability of the information system, plus the acceptable verification of the implementation and performance of IA controls assigned.

d. Ensure information systems under his/her purview are reaccredited prior to the termination of an existing authorization to operate (ATO) or interim authorization to operate (IATO).

e. Ensure that all users are provided training on the secure use of the information system prior to being granted access. User training shall be structured to reflect the different user roles and privileges (e.g., system administrator, database administrator, and application user). Where applicable, IA rules of behavior specific to each information system shall be developed in accordance with DLAI 6404 (Reference (h)).

f. Ensure that positions responsible for performing IA and IT functions for information systems under his/her purview are designated the applicable IT level (i.e., IT-I, IT-II, and IT-III, in accordance with Reference (b). DOD civilian, military (active duty and reservist), and contractor personnel occupying these positions shall undergo the appropriate personnel security investigation as prescribed by DOD 5200.2-R (Reference (i)) and Reference (b) prior to his/her assignment.

5. PM/SM. The PM/SM shall:

a. Ensure the execution of the DIACAP in accordance with the DLA DIACAP Implementation Guide for all assigned DLA information systems.

b. Ensure information systems under his/her purview are registered in eMASS at the inception of the C&A process.

c. Plan for IA control implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

d. Ensure that an information system security engineer is assigned to implement or modify the IA components of any given information system's architecture for which he/she is responsible.

e. Budget for IA design, implementation, validation and sustainment throughout the system life cycle utilizing DLA Financial Operations Information Technology (FOIT), Section 4.B. to sustain the information system's security posture at an acceptable level

f. Ensure an appointed DLA IAM, to include an appointed alternate IAM, is assigned with the support, authority, and resources necessary to satisfy his/her responsibilities. This includes ensuring all IAMs are appointed in writing as prescribed herein prior to assigning the IAM role for information systems under his/her purview.

g. Ensure an appointed and assigned Information Assurance Officer (IAO), to include an alternate IAO, for all information systems under his/her purview. The appointment shall be in writing, and a file copy maintained for reference. All appointed IAO's shall acknowledge their assigned roles and responsibilities through signature.

h. Ensure that qualified and properly trained IA and IT personnel utilize only authorized automated IA tools (e.g., Retina scans, Web Inspect, etc.) to assess the adequacy and proper configuration of information systems and assigned IA controls.

i. Maintain IA related situational awareness with respect to information systems under his/her purview.

6. IAM. The IAM shall:

a. For information systems under his/her purview, ensure that the information systems and operating environments are continuously monitored for security relevant events and configuration changes that may negatively impact its accredited IA posture.

b. Support the responsible PM/SM in implementing the objectives of all assigned IA controls for information systems under his/her purview.

c. For information systems under his/her purview, notify the DLA CA of any changes affecting the IA posture of any accredited information system under the purview of the DLA DAA.

d. Track and oversee all corrective or mitigating actions for weaknesses and identify in POA&M's for information systems under his/her purview.

e. Be responsible for the oversight of annual IA control reviews for accredited (ATO) information systems under his/her purview

7. IAO. The IAO shall:

a. Ensure that DIACAP packages for information systems under his/her purview are developed and provided to the responsible IAM for review and approval.

b. Notify the responsible IAM when changes are requested or planned for information systems that might affect that system's IA posture.

ENCLOSURE 3

PROCEDURES

1. CERTIFICATION. The PM/SM and CA Representative make a certification recommendation and the CA renders a certification decision for the information system in eMASS.

a. The PM/SM:

(1) Registers emerging and operational information systems in eMASS to initiate the C&A process.

(2) Considers the information system's accreditation boundary, scope, and deployment strategy when selecting the information system type (automated information system application, enclave, platform IT (PIT) interconnection, or outsourced IT-based business process) and appropriate C&A methodology (e.g., Type Accreditation, etc.).

(3) Assigns a Mission Assurance Category (MAC) and Confidentiality Level (CL) (e.g., public, sensitive, classified) for all information systems under his/her purview.

b. The IAO, in conjunction with the applicable validation personnel (e.g., system administrators, database administrators, security engineers), conducts validation testing of applicable IA controls for emerging information systems and at least annually for operational systems under his/her purview to ensure conformance with the stated IA control objectives.

c. The CA Representative:

(1) In conjunction with the responsible PM/SM and IAM, ensures that all identified non-compliant IA controls are assessed to determine the likelihood of information system-wide exploits of the identified weaknesses.

(2) Ensures that identified weaknesses that cannot be corrected immediately are included in a POA&M that identifies tasks to be accomplished in order to resolve those identified weaknesses (e.g., non-compliant IA controls and baseline IA controls that are not applicable because of the nature of the system, e.g., stand-alone) as part of a new or existing DIACAP package.

(a) The POA&M format along with instructions are provided in Reference (g), and in the POA&M section of the DIACAP Knowledge Service (KS).

(b) All requests for an IATO shall be accompanied by a POA&M that documents identified weaknesses and specifies correcting or mitigating actions that are feasible and achievable within the authorization period.

(3) Ensures that the applicable Severity Category (e.g., CAT I, II, III) is assigned to all weaknesses documented in the corresponding POA&M. The CAT shall be assigned to a weakness by the CA Representative to indicate the level of risk and the urgency with which corrective security measures shall be implemented.

(a) Mark as "Not Applicable" within the "Resources Required", "Scheduled Completion Date", "Milestones with Completion Dates", and "Milestone Changes" columns in the POA&M when an acceptance of risk is requested for a CAT III weakness (e.g., technology limitations, prohibitive costs).

(b) Mark with "Risk Accepted by DAA" in the "Status" column once the risk is accepted by the DAA.

(c) Provide in the "Comments" column a short summary of the rationale for requesting the acceptance of risk and upload an artifact into eMASS providing the complete rationale and risk analysis, if applicable.

2. ACCREDITATION PROCESS. The DAA renders an accreditation decision for the information system in eMASS based on certification results, business requirements, and mission impact. Accreditation decisions result in one of the following authorizations: ATO, IATO, Interim Authorization to Test (IATT), or Denial of Authorization to Operate (DATO). The DAA may:

a. Grant an ATO for a period not to exceed three (3) years in duration or an IATO for a period not to exceed 180 days at any given time and issuances of consecutive IATO's shall not total more than 360 days.

(1) Information systems with an identified Severity Category (CAT) I weakness (Severity Categories are discussed in DLA DIACAP Implementation Guide, (Reference (g), Section 7.5.4.3) (this shall be confirmed through analysis of the risk presented by the weakness) that has not been successfully mitigated or corrected shall not be granted an ATO.

(2) A DLA information system can be issued an IATO with a CAT I weakness only when it is critical to military operations as determined by affected executive director(s) or commander(s), and if failure to deploy or allow continued operation of the deployed information system shall preclude mission accomplishment.

(3) The approved operation of the information system shall follow a request by the affected executive director(s) or military commander(s) and a copy of an authorization memorandum with supporting rationale shall be provided to the DOD SIAO.

b. Consult with the responsible J6 Director (if applicable), IT chief, PM/SM, or business area manager, prior to issuing a DATO or denying an IATT request to ascertain any possible adverse mission and/or business related impacts that could result from the DAA's decision.

c. Grant an ATO for a DLA information system with an identified CAT II weakness only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.

d. Authorize continued operation of an information system under an IATO in which CAT II weaknesses have not been corrected or successfully mitigated within a 360 day time frame (e.g., two consecutive 180 day IATO's); but, the DAA shall certify in writing that continued operation of the DLA information system is critical to mission accomplishment, and a copy of the authorization with supporting rationale shall be provided to the DOD SIAO.

e. Grant information systems with CAT III weaknesses an ATO at his/her discretion. The DAA shall determine if CAT III weaknesses shall be corrected or the risk accepted.

f. Downgrade an ATO and assignment of an IATO. Factors that can result in the DAA downgrading include, but are not limited to:

(1) Failure to complete and provide substantiation of mandated annual exercises or drills as they relate to continuity of operations planning in accordance with IA control COED-1/2;

(2) Failure to ensure the proper storage of backup copies of critical software in accordance with IA control, COSW-1;

(3) Significant changes in the information system's functional design, architecture, environment, or sensitivity of data processed; or

g. Rescind a previous ATO and disconnection from the live production environment. Factors that can result in the DAA rescinding an ATO and disconnection can include, but are not limited to:

(1) Failure to complete a documented POA&M milestone within the required timeframe;

(2) Detection of a new CAT I weakness that cannot be mitigated to a minimally accepted level of risk; or

(3) A security incident resulting in the compromise of sensitive data.

h. Ensure that corrective and mitigating actions identified in all active POA&M's for DLA information systems with an ATO or an IATO are monitored and tracked through to resolution or to the point that an acceptable level of risk is achieved for identified weaknesses.

3. CONTINUOUS ASSESSMENT OF RISK.

a. The CA Representative and PM/SM, in conjunction with the assigned IAM, ensure that corrective and mitigating actions identified in all active POA&M's for DLA information systems

with an ATO or an IATO are monitored and tracked through to resolution or to the point that an acceptable level of risk is achieved for identified weaknesses and annual IA control reviews are conducted in accordance with the Reference (g).

b. The IAO, in conjunction with the applicable validation personnel (e.g., system administrators, database administrators, security engineers), at least annually conducts validation testing of applicable IA controls for information systems under his/her purview to ensure conformance with the stated IA control objectives.

c. The IAM:

(1) Shall ensure that procedures are in place to facilitate IT resources (e.g., hardware, software, documentation, support personnel) in support of J6 sponsored IA Compliance Reviews and all other applicable, internal and external reviews/assessments (e.g., third-party penetration testing, Red Team exercises, etc.) of information systems under his/her purview. Corrective or mitigating actions documented in POA&M's and other reports as a result of a DLA IA Compliance Review or any other applicable internal or external review/assessment shall be tracked and managed through to resolution.

(2) Shall provide a written statement endorsed by the CA Representative, or if there is no presiding CA Representative the PM/SM, attesting to the results of the annual IA control review conducted in accordance with the Reference (g).

d. The CA Representative shall ensure that :

(1) A continuous risk management process throughout the life cycle of the information systems under his/her purview is implemented. The continuous risk management process should result in the continuous assessment of the risk posed by new and existing weaknesses in order to identify and implement appropriate controls to correct and/or satisfactorily mitigate the information system's risk of exploitation.

(2) In conjunction with ensuring the annual review of all applicable IA controls assigned to the information system, endorse a written statement confirming the effectiveness of assigned IA controls and their implementation or recommending applicable changes to ensure their effectiveness.

(3) IA and IT personnel utilize formal and informal reports (e.g., Retina scan reports, intrusion detection system logs, Security Readiness Review scan and checklist results, Federal audit reviews (e.g., General Accountability Office (GAO) audit reports, Federal Information System Controls Audit Management (FISC) reports)and DLA IA Compliance Review reports) to identify and correct, or satisfactorily mitigate, identified weaknesses.

(4) The implementation of a change management and configuration management process, to manage the potential IA impacts resulting from changes to information systems and/or their supporting infrastructure throughout the life cycle. All proposed changes to the

information system affecting the IA baseline shall be assessed for risks to the DLA IT enterprise and the Global Information Grid (GIG).

(5) CM procedures are developed and implemented to control and maintain an accurate inventory of IT resources (e.g., system hardware, software, and firmware components).

(6) Information system change requests are reviewed to assess the potential impact on the information system's IA posture.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ATO	authorization to operate
C&A	certification and accreditation
CA	certifying authority
CAT	category
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
CL	confidentiality level
CM	change management/configuration management
DAA	designated accrediting authority
DATO	denial of authorization to operate
DIACAP	DOD information assurance certification and accreditation process
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DLAI	Defense Logistics Agency Instruction
DODD	DOD Directive
DODI	DOD Instruction
eMASS	Enterprise Mission Assurance Support Service
FISC	Federal Information System Controls
FISMA	Federal Information Security Management Act
FOIT	Financial Operations Information Technology
GAO	General Accounting Office
GIG	Global Information Grid
KS	Knowledge Service
J6	Information Operations
J61	Compliance Management & IT Operations Support Services
IA	information assurance
IAM	information assurance manager
IAO	information assurance officer
IATO	interim authorization to operate
IATT	interim authorization to test
IT	information technology
MAC	Mission Assurance Category

NIPRNet	non-classified internet protocol router network
PIT	platform IT interconnection
PM	program manager
POA&M	plan of actions and milestones
SIAO	senior information assurance officer
SIPRNet	secret internet protocol router network
SM	system manager
STIGS	Security Technical Implementation Guides
TAG	technical advisory group
WIP	Workforce Improvement Program
USCYBERCOM	United States Cyber Command